

In herkömmlichen DSL-Zugangsnetzen erfolgt die Anbindung des DSLAM an nachgeordnete Netzelemente mittels eines ATM-Netzwerkes (ATM=Asynchronous Transfer Mode, asynchroner Transfermodus).

5

Nachteilig ist dabei, daß ATM-Netzwerke sowohl beim Aufbau als auch im Betrieb teuer und aufwendig sind, da einerseits die Komponenten eines ATM-Netzwerkes (z.B. Switches) im Vergleich zu Komponenten, die andere Übertragungstechniken unterstützen, teuer sind und andererseits jede Verbindung eines ATM-Netzwerkes gesondert administriert werden muss.

Um diesen Nachteil zu umgehen, wird beispielsweise in "DSL: The Corporate Connection", T. Jessup, Data Communications Bd. 27, Nr. 2 (Februar 1998), S. 103-108, McGraw Hill, New York, vorgeschlagen, die DSL Zugangsleitungen mit ATM-Netzen, Ethernets, T1-Verbindungen, seriellen Leitungen oder Frame Relay zu verbinden.

20 Erfolgt die teilnehmerseitige Terminierung der Verbindung kostengünstig mittels Ethernet, besteht jedoch die Gefahr, dass aufgrund der Selbstkonfigurationsfähigkeiten der im Zusammenhang mit dem Zugangsmultiplexer DSLAM erforderlichen Ethernet-Bridge ein Angriff auf den DSLAM mit einer großen Anzahl 25 gefälschter MAC-Adressen (MAC=Media Access Control) die Routing-Tabellen des DSLAM zum Überlauf bringt. Außerdem sind bei ungefiltertem Ethernet-Verkehr beispielsweise unautorisierte Verbindungen zwischen den Datenendgeräten D1, D2, D3 möglich.

30 Es ist daher eine Aufgabe der vorliegenden Erfindung, ein Verfahren und einen Zugangsmultiplexer für den schnellen Zugang zu Datennetzen anzugeben, durch welche Angriffe auf einen DSLAM verhindert und unautorisierte Direktverbindungen 35 zwischen am DSLAM angeschlossenen Datenendgeräten unterbunden werden.

Diese Aufgabe wird durch ein Verfahren für den schnellen Zugang zu Datennetzen ausgehend vom Oberbegriff des Patentanspruchs 1 durch dessen kennzeichnende Merkmale und einen Zugangsmultiplexer für den schnellen Zugang zu Datennetzen ausgehend vom Oberbegriff des Patentanspruchs 7 durch dessen kennzeichnende Merkmale gelöst.

Bevorzugte Ausführungsformen sind Gegenstand der abhängigen Ansprüche.

10

Gemäß der vorliegenden Erfindung wird ein Verfahren für den schnellen Zugang zu Datennetzen INT vorgesehen, bei dem Datenendgeräte D1, D2, D3 von Teilnehmern mittels je eines Modems M1, M2, M3 über je eine digitale Teilnehmeranschlussleitung DSL1, DSL2, DSL3 mit einem Zugangsmultiplexer DSLAM verbunden sind, wobei zur Datenübertragung zwischen den Datenendgeräten D1, D2, D3 und einem dem Zugangsmultiplexer (DSLAM) nachgeordneten Zugriffsserver B-RAS, durch welchen die Zugriffsberechtigung der Datenendgeräte D1, D2, D3 überprüft und der Zugriff auf das Datennetz (INT) hergestellt wird, das Point-to-Point-Protocol over Ethernet PPPoE eingesetzt wird, wobei die Anbindung des Zugangsmultiplexers DSLAM an den Zugriffsserver B-RAS und an weitere nachgeordnete Komponenten mittels eines Ethernet-Netzwerkes ETH erfolgt. Dabei weist der Zugangsmultiplexer eine Ethernet-Bridge auf, die Filtermittel zum Auswerten der in empfangenen Ethernet-Rahmen enthaltenen PPPoE-Header aufweist, wobei:

- Ethernet-Rahmen an die Ethernet-Bridge (EB) weitergeleitet werden, wenn der PPPoE-Header einer bestehenden, durch den Zugriffsserver (B-RAS) bestätigten Verbindung zuordenbar ist oder wenn der PPPoE-Header einem Verbindungsauflauf zuordenbar ist, und
- alle anderen Ethernet-Rahmen, die einen PPPoE-Header enthalten, verworfen werden, und
- alle Ethernet-Rahmen, die keinen PPPoE-Header enthalten, verworfen werden.

3A

Mit anderen Worten werden alle Ethernet-Rahmen verworfen, die nicht einer bestehenden PPPoE-Verbindung oder einem PPPoE-Verbindungsaufbau zuordenbar sind.

5 Gemäß der vorliegenden Erfindung wird außerdem ein Zugangs-
multiplexer DSLAM für den schnellen Zugang zu Datennetzen INT
vorgesehen, an den Datenendgeräte D1, D2, D3 von Teilnehmern
mittels je eines Modems M1, M2, M3 über je eine digitale
Teilnehmeranschlussleitung DSL1, DSL2, DSL3 angeschlossen
10 sind, wobei zur Datenübertragung zwischen den Datenendgeräten
D1, D2, D3 und einem Zugriffsserver B-RAS, durch welchen die
Zugriffsberechtigung der Datenendgeräte D1, D2, D3 überprüft
und der Zugriff auf das Datennetz (INT) hergestellt wird, das
Point-to-Point-Protocol over Ethernet PPPoE eingesetzt wird,
15 wobei der Zugangsmultiplexer DSLAM mit dem Zugriffsserver (B-
RAS) und mit weiteren nachgeordneten Komponenten mittels ei-
nes Ethernet-Netzwerkes (ETH) verbunden ist und wobei der Zu-
gangsmultiplexer die o.g. Ethernet-Bridge und Filtermittel
aufweist.
20 Ein wichtiger Vorteil des erfindungsgemäßen Verfahrens und
des erfindungsgemäßen Zugangsmultiplexers DSLAM besteht dar-
in, dass der Aufbau eines Ethernet-Netzwerkes erheblich ko-
stengünstiger ist als der Aufbau eines ATM-Netzwerkes, da
25 Ethernet-Komponenten einfacher und damit kostengünstig her-
stellbar sind. Wartung und Betrieb eines Ethernet-Netzwerkes
sind ebenfalls deutlich kostengünstiger, da ein Ethernet-
Netzwerk selbstkonfigurierend ist und somit die bei ATM-
Netzwerken erforderliche Administration des Netzwerkes ent-
30 fällt. Dabei wird durch die Erfindung verhindert, daß
Angriffe auf einen DSLAM z.B. mittels gefälschter MAC-Adres-
sen ausgeführt werden können und daß unautorisierte
Direktverbindungen zwischen am DSLAM angeschlossenen
Datenendgeräten aufgebaut werden können.
35 ...

Vorteilhaft bleibt bei Anwendung der Erfindung die herkömmliche Anbindung der Datenendgeräte der Teilnehmer an den Zugangsmultiplexer bestehen.

- 5 In einer Weiterbildung des erfindungsgemäßen Verfahrens und des erfindungsgemäßen Zugangsmultiplexers wird eine Kombination mit einem Verfahren bzw. Mitteln zur Überlastabwehr vorgesehen - Ansprüche 3 bis 5 und 9 bis 11. Der Vorzug dieser Kombination besteht darin, dass starke Impulse bzw. Bursts
- 10 von Datenverkehr auf der hochbitratigen Ethernet-Schnittstelle, die an nur eine der - im Vergleich zu der Ethernet-Schnittstelle niederbitratigen -digitalen Teilnehmeranschlussleitungen weiterzuleiten sind, dort nicht zu einer Überlastsituation führen können, da erforderlichenfalls
- 15 Ethernet-Rahmen bereits aus dem Empfangspuffer der Ethernet-Schnittstelle verworfen werden. Vorteilhaft werden Ethernet-Rahmen, die der Verbindungssteuerung dienen, von der Verwurfsstrategie ausgenommen.
- 20 Im folgenden wird das erfindungsgemäße Verfahren im Zusammenhang mit einer Zeichnung als Ausführungsbeispiel näher erläutert.

Die einzige Figur 1 zeigt schematisch den Netzaufbau für einen schnellen Zugang zu einem Datennetz mittels digitaler Teilnehmeranschlussleitung.

Figur 1 zeigt drei Datenendgeräte D1, D2, D3, mittels je eines Modems M1, M2, M3 über je eine digitale Teilnehmeranschlussleitung DSL1, DSL2, DSL3 mit einem Zugangsmultiplexer

Patentansprüche

1. Verfahren für den schnellen Zugang zu Datennetzen (INT), bei dem Datenendgeräte (D1, D2, D3) von Teilnehmern mittels je eines Modems (M1, M2, M3) über je eine digitale Teilnehmeranschlussleitung (DSL1, DSL2, DSL3) mit einem Zugangsmultiplexer (DSLAM) verbunden sind, wobei zur Datenübertragung zwischen den Datenendgeräten (D1, D2, D3) und einem dem Zugangsmultiplexer (DSLAM) nachgeordneten Zugriffsserver (B-RAS), durch welchen die Zugriffsberechtigung der Datenendgeräte (D1, D2, D3) überprüft und der Zugriff auf das Datennetz (INT) hergestellt wird, das Point-to-Point-Protocol over Ethernet PPPoE eingesetzt wird, und wobei die Anbindung des Zugangsmultiplexers (DSLAM) an den Zugriffsserver (B-RAS) und an weitere nachgeordnete Komponenten mittels eines Ethernet-Netzwerkes (ETH) erfolgt,
dadurch gekennzeichnet,
dass eine Ethernet-Bridge (EB) dem Zugangsmultiplexer (DSLAM) zugeordnet oder in den Zugangsmultiplexer (DSLAM) integriert wird, wobei die Ethernet-Bridge (EB) mit Filtermitteln ausgerüstet wird, durch welche die in empfangenen Ethernet-Rahmen enthaltenen PPPoE-Header ausgewertet werden und wobei:
 - Ethernet-Rahmen an die Ethernet-Bridge (EB) weitergeleitet werden, wenn der PPPoE-Header einer bestehenden, durch den Zugriffsserver (B-RAS) bestätigten Verbindung zuordenbar ist oder wenn der PPPoE-Header einem Verbindungsaufbau zuordenbar ist und
 - alle anderen Ethernet-Rahmen, die einen PPPoE-Header enthalten, verworfen werden, und
 - alle Ethernet-Rahmen, die keinen PPPoE-Header enthalten, verworfen werden.
2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,
dass mit dem Verbindungsaufbau ein Timer gestartet wird,

5 bei dessen Ablauf die MAC-Adresse der sendenden Ethernet-Komponente aus den Routing-Tabellen der Ethernet-Bridge (EB) entfernt wird, sofern vor Ablauf des Timers keine Bestätigung des Verbindungsaufbaus durch den Zugriffsserver (B-RAS) erfolgt.

7. Zugangsmultiplexer (DSLAM) für den schnellen Zugang zu 10 Datennetzen (INT), an den Datenendgeräte (D1, D2, D3) von Teilnehmern mittels je eines Modems (M1, M2, M3) über je eine digitale Teilnehmeranschlussleitung (DSL1, DSL2, DSL3) angeschlossen sind, wobei zur Datenübertragung zwischen den Datenendgeräten (D1, D2, D3) und einem dem Zugangsmultiplexer (DSLAM) nachgeordneten Zugriffsserver (B-RAS), 15 durch welchen die Zugriffsberechtigung der Datenendgeräte (D1, D2, D3) überprüft und der Zugriff auf das Datennetz (INT) hergestellt wird, das Point-to-Point-Protocol over Ethernet PPPoE eingesetzt wird, und wobei der Zugangsmultiplexer (DSLAM) mit dem Zugriffsserver (B-RAS) und mit weiteren nachgeordneten Komponenten mittels 20 eines Ethernet-Netzwerkes (ETH) verbunden ist, dadurch gekennzeichnet, dass der Zugangsmultiplexer eine Ethernet-Bridge (EB) 25 aufweist, wobei die Ethernet-Bridge (EB) Filtermittel zum Auswerten der in empfangenen Ethernet-Rahmen enthaltenen PPPoE-Header aufweist, und wobei:

- 30 Ethernet-Rahmen an die Ethernet-Bridge (EB) weitergeleitet werden, wenn der PPPoE-Header einer bestehenden, durch den Zugriffsserver (B-RAS) bestätigten Verbindung zuordenbar ist oder wenn der PPPoE-Header einem Verbindungsauftbau zuordenbar ist, und
- alle anderen Ethernet-Rahmen, die einen PPPoE-Header enthalten, verworfen werden, und
- alle Ethernet-Rahmen, die keinen PPPoE-Header enthalten, 35 verworfen werden.

8. Zugangsmultiplexer (DSLAM) nach Anspruch 7, der zusätzlich einen Timer aufweist, der mit dem Verbindungsauftbau gestartet wird, bei dessen Ablauf die MAC-Adresse der sendenden Ethernet-Komponente aus den Routing-Tabellen der Ethernet-Bridge (EB) entfernt wird, sofern vor Ablauf des Timers keine Bestätigung des Verbindungsauftbaus durch den Zugriffsserver (B-RAS) erfolgt.

In conventional DSL access networks, the DSLAM is linked to downstream network elements by means of an ATM network (ATM = asynchronous transfer mode).

5

The disadvantage in this situation is the fact that ATM networks are expensive and complicated both in their construction and in their operation since on the one hand the components of an ATM network (switches for example) are expensive in comparison with components which support other transfer technologies and on the other hand each connection in an ATM network needs to be administered separately.

10

In order to avoid this disadvantage, "DSL: The Corporate Connection", T. Jessup, Data Communications Vol. 27, No. 2 (February 15 1998), pp. 103-108, McGraw Hill, New York, proposes for example that the DSL access lines be connected using ATM networks, Ethernets, T1 connections, serial lines or frame relays.

If the subscriber-side termination of the connection is implemented 20 cost-effectively using Ethernet, there is however a danger that as a result of the self-configuration capabilities of the Ethernet bridge

EB required in conjunction with the access multiplexer DSLAM an attack on the DSLAM using a large number of falsified MAC addresses (MAC = media access control) causes the routing tables of the DSLAM 25 to overflow. In addition, in the case of unfiltered Ethernet traffic, unauthorized connections between the data terminal devices D1, D2, D3 are possible, for example.

The object of the present invention is therefore to specify a method

30 and an access multiplexer for quick access to data networks, by means of which attacks on a DSLAM are prevented and unauthorized direct connections between data terminal devices connected to the DSLAM are prevented.

35

This object is achieved by a method for quick access to data networks on the basis of the preamble of Claim 1 through its characterizing features, and by an access multiplexer for quick access to data networks on the basis of the preamble of Claim 7 5 through its characterizing features.

Preferred embodiments are set down in the dependent claims.

According to the present invention, a method for quick access to 10 data networks INT is provided in which data terminal devices D1, D2, D3 of subscribers are each connected by means of a modem M1, M2, M3 respectively by way of a digital subscriber line DSL1, DSL2, DSL3 respectively to an access multiplexer DSLAM, whereby for the purposes of data transfer between the data terminal devices D1, D2, 15 D3 and an access server B-RAS which is located downstream of the access multiplexer (DSLAM), which serves to check the access authorization of the data terminal devices D1, D2, D3 and establish the access to the data network (INT), the Point-to-Point Protocol over Ethernet PPPoE is used, according to which the link from the 20 access multiplexer DSLAM to the access server B-RAS and to further components located downstream is implemented by means of an Ethernet network ETH. In this situation the access multiplexer has an Ethernet bridge (EB) which has filtering facilities for evaluating the PPPoE headers contained in received Ethernet frames, whereby: 25

- Ethernet frames are routed to the Ethernet bridge (EB) if the PPPoE header can be assigned to an existing connection confirmed by the access server, or if the PPPoE header can be assigned to connection which is set up, and
- all other Ethernet frames which contain a PPPoE header are 30 discarded, and
- all Ethernet frames which do not contain a PPPoE header are discarded.

3A

In other words, all those Ethernet frames are discarded which can not be assigned to an existing PPPoE connection or to a PPPoE connection which is set up.

- 5 In accordance with the present invention, for quick access to data networks INT an access multiplexer DSLAM is additionally provided, to which data terminal devices D1, D2, D3 of subscribers are each connected by means of a modem M1, M2, M3 respectively by way of a digital subscriber line DSL1, DSL2, DSL3 respectively, whereby for
- 10 the purposes of data transfer between the data terminal devices D1, D2, D3 and an access server B-RAS, which serves to check the access authorization of the data terminal devices D1, D2, D3 and establish the access to the data network (INT), the Point-to-Point Protocol over Ethernet PPPoE is used, whereby the access multiplexer DSLAM is
- 15 connected to the access server (B-RAS) and to further components located downstream by means of an Ethernet network (ETH) and whereby the access multiplexer has the aforementioned Ethernet bridge and filtering facilities.
- 20 An important advantage of the method according to the invention and of the access multiplexer DSLAM according to the invention consists in the fact that it is considerably more cost-effective to set up an Ethernet network than to set up an ATM network since Ethernet components are simpler and thus cheaper to manufacture. Maintenance
- 25 and operation of an Ethernet network are likewise significantly more cost-effective since an Ethernet network is self-configuring and the network administration required in the case of ATM networks is thus dispensed with. In this situation, the invention prevents attacks from being carried out on a DSLAM, using falsified MAC addresses for
- 30 example, and prevents the possibility of unauthorized direct connections being set up between data terminal devices connected to the DSLAM.

Advantageously, when using the invention the conventional link between the data terminal devices of the subscribers and the access multiplexer is retained.

5

In one development of the method according to the invention and of the access multiplexer according to the invention, a combination with a method and/or with means offering overload protection is provided - Claims 3 to 5 and 9 to 11. The advantage of this

10 combination consists in the fact that strong pulses or bursts of data traffic on the high bit rate Ethernet interface, which are to be routed to only one of the digital subscriber lines - which are low bit rate when compared with the Ethernet interface -, can not result in an overload situation there since Ethernet frames are
15 necessarily already discarded from the receive buffer of the Ethernet interface. Ethernet frames which are used for connection control are advantageously excluded from the discard strategy.

20 The method according to the invention will be described in detail in the following as an embodiment with reference to a drawing.

The single Figure 1 shows a schematic view of the network structure for quick access to a data network using a digital subscriber line.

25 Figure 1 shows three data terminal devices D1, D2, D3 which are each connected by means of a modem M1, M2, M3 respectively by way of a digital subscriber line DSL1, DSL2, DSL3 respectively to an access multiplexer DSLAM.

Claims

1. Method for quick access to data networks (INT), in which data

5 terminal devices (D1, D2, D3) of subscribers are each connected by means of a modem (M1, M2, M3) respectively by way of a digital subscriber line (DSL1, DSL2, DSL3) respectively to an access multiplexer (DSLAM), whereby for the purposes of data transfer between the data terminal devices (D1, D2, D3) and an access 10 server (B-RAS) which is located downstream of the access multiplexer (DSLAM), which serves to check the access authorization of the data terminal devices (D1, D2, D3) and establish the access to the data network (INT), the Point-to-Point Protocol over Ethernet PPPoE is used, and whereby the link 15 from the access multiplexer (DSLAM) to the access server (B-RAS) and to further components located downstream is implemented by means of an Ethernet network (ETH)

characterized in that

an Ethernet bridge (EB) is assigned to the access multiplexer

20 (DSLAM) or is integrated into the access multiplexer (DSLAM), whereby the Ethernet bridge (EB) is equipped with filtering facilities through which the PPPoE headers contained in received Ethernet frames are evaluated and whereby:

- Ethernet frames are routed to the Ethernet bridge (EB) if the 25 PPPoE header can be assigned to an existing connection confirmed by the access server, or if the PPPoE header can be assigned to connection which is set up, and
- all other Ethernet frames which contain a PPPoE header are discarded, and
- all Ethernet frames which do not contain a PPPoE header are 30 discarded.

2. Method according to Claim 1,

characterized in that

35 a timer is started when the connection is set up and when the

timer times out the MAC address of the sending Ethernet component is removed from the routing tables of the Ethernet bridge (EB) provided that no confirmation of the connection set-up is given by the access server (B-RAS) before the timer times out.

5

7. Access multiplexer (DSLAM) for quick access to data networks (INT), to which data terminal devices (D1, D2, D3) of subscribers are each connected by means of a modem (M1, M2, M3) respectively by way of a digital subscriber line (DSL1, DSL2, DSL3)

10 respectively, whereby for the purposes of data transfer between the data terminal devices (D1, D2, D3) and an access server (B-RAS) which is located downstream of the access multiplexer (DSLAM), which serves to check the access authorization of the data terminal devices (D1, D2, D3) and establish the access to 15 the data network (INT), the Point-to-Point Protocol over Ethernet PPPoE is used, and whereby the access multiplexer (DSLAM) is connected to the access server (B-RAS) and to further components located downstream by means of an Ethernet network (ETH), characterized in that

20 the access multiplexer has an Ethernet bridge (EB), whereby the Ethernet bridge (EB) has filtering facilities for evaluating the PPPoE headers contained in received Ethernet frames, and whereby:

- Ethernet frames are routed to the Ethernet bridge (EB) if the PPPoE header can be assigned to an existing connection confirmed 25 by the access server, or if the PPPoE header can be assigned to connection which is set up, and
- all other Ethernet frames which contain a PPPoE header are discarded, and
- all Ethernet frames which do not contain a PPPoE header are 30 discarded.

8. Access multiplexer (DSLAM) according to Claim 7, additionally comprising a timer which is started when the connection is set up and when the timer times out the MAC address of the sending Ethernet component is removed from the routing tables of the 5 Ethernet bridge (EB) provided that no confirmation of the connection set-up is given by the access server (B-RAS) before the timer times out.